Privacy labelling, enhancing the competitiveness of SMEs

Josef Noll, (on behalf of the SCOTT team)
Secure Connected Trustable Things key message

IoT is the game changer and driver for digitalisation, and SCOTT contributes through:

- Answer the IoT need for a new and more advanced security paradigm through security classes
- Create a Convincing privacy assessment through privacy labelling
- Establish a clear link between security and safety
The answer to security

There will be no peace until all men learn to understand each other.

True...

How are we going to get everybody to speak Norwegian?

Teach our sensors to talk Norwegian.
The trust matrix

- trust as a positive user attitude
  - engaging voluntarily
- security based trust issues
  - building trusted systems
- technological factors
  - data storage, distribution
  - insight
- human/societal factors
  - government
  - family, friends

http://SCOTT.IoTSec.no
http://SCOTT-project.eu
Privacy labelling (A-F)
- declare the level of privacy of devices and services
The economic perspective

- The big 5 IT companies have a GDP as big as that of France
- Amazon largest sector in terms of revenue is selling of data
  - 20% of revenue

How can SMEs compete?
- Each service and device gets a privacy label

Four areas for Privacy Label
- which data are collected
- sharing to my phone, my cloud, public cloud,…
- data communication integrity and storage
- further distribution of data, ownership of data, further processing

Privacy Label (A-F)
- easy visibility
- customer focus
- transparent

Privacylabel.IoTSec.no
“Measure, what you can measure - Make measurable, what you can’t measure” - Galileo

Privacy today
- based on lawyer terminology
- 250,000 words on app terms and conditions

Privacy tomorrow
- A++: sharing with no others
- A: ...
- C: sharing with ....

The Privacy label for apps and devices
Privacy Label (A-F) - ongoing discussion

Level A++
- no data are shared

Level A+

Level A - Very high
- restricted use of data to purpose only (particular service)
- supplier should bear the risk of incidents, e.g. they rather than I get penalised when things go wrong - equivalent to finansavtaleloven
- if device is stolen - nobody else

Level B
- specify the data to be collected, re-use for statistical data only, ensured integrity
- customizable access control, e.g. add stronger authentication or consent requirements
- must be able to trade off the various security requirements, e.g. confidentiality against availability - i.e. I want flexibility
- compliance with other standards - and this be listed (information requirement) - clipper compatible
- anonymity of my interaction with the supplier
- customer can control with how the information is transferred and used by a third party

Level C
- data are collected without control (GPS+activity+heart rate), re-use only for statistical, encrypted storage
- must be possible to withdraw consent - and that this results in all relevant information being deleted - and proof of deletion

Level D
- data are collected, transparency of re-use
- Data is not sold without consent/knowledge
- transparency - I get told about the criteria that the supplier has used in their information classification
- Information is only used for its legitimate purpose

Level E
- collected data, no transparency of re-use
- in compliance with GDPR
- if data is stolen, I will get told
- notification if DSO is hacked

Level F - Failure
- no privacy, no control of data, everyone can see
- nothing, no expectations
Answer the Challenges addressed by the EU

DIGITALEUROPE’s views on Cybersecurity Certification and Labelling Schemes

*Brussels, 23 March 2017*

**RECENT EU PROPOSALS ON CYBERSECURITY CERTIFICATION AND LABELLING**

In the course of 2016 the European Commission announced two initiatives for further assessment in the field of certification and labelling: 1) a security certification framework for ICT products and 2) a “Trusted IoT label” giving information about different levels of privacy and security and, where relevant, demonstrating compliance with the NIS Directive.

2. Trusted IoT Label

In its July 2016 Communication, the European Commission also brought forward the idea of a European label for trust/security of ICT products. This has since been further elaborated in policy discussions in the context of the Internet of Things ("IoT") and has been suggested as a potential item for a Trust in the Digital Single Market package in the Spring 2017.

SCOTT contribution: privacy label?
Discussion
- privacy label
- levels A-F
- competitive advantage